I Claim:

1. (Amended) A system for authenticating an encryption key of a user, comprising: a decrypt engine for using a password provided by the user to decrypt an encrypted data file provided by the user into the encryption key of the user.

2. (Amended) The system of claim 1, wherein the encrypted data file is stored on an RF smart card.

3. (Amended) The system of claim 1, wherein the encrypted data file includes encrypted biometric data identifying the user.

7. (Amended) A method for providing an authenticated encryption key of a user, comprising the steps of:

providing an encrypted data file;

providing a password; and

decrypting the encrypted data file, using the password, into an authenticated encryption key of the user.

8. (Amended) The method of claim 7, wherein the encrypted data file is stored on an RF smart card.

9. (Amended) The method of claim 7, wherein the encrypted data file includes encrypted biometric data identifying the user.

10. The method of claim 9, wherein the biometric data includes a digitized fingerprint of the user.

11. (Amended) The method of claim 7, further including the steps of:

generating biometric data of the user by scanning a biometric feature of the user; and

probabilistically comparing the generated biometric data of the user to data derived from the encrypted data file to authenticate the encryption key of the user.

12. The method of claim 11, wherein the scanned biometric feature of the user is a fingerprint.

13. (Amended) A computer-accessible medium comprising program instructions for providing an authenticated encryption key of a user, by performing the step of:

using a password provided by the user to decrypt an encrypted data file provided by the user into an authenticated encryption key of the user.

14. (New) The system of claim 1, wherein the encrypted data file includes encrypted biometric data, derived from a digitized fingerprint of the user, identifying the user.

15. (New) The system of claim 1, further comprising a biometric reader for generating a first biometric data of the user, wherein the first biometric data of the user is compared with a second biometric data of the user stored in the encrypted data file.

16. (New) The system of claim 1, further comprising a fingerprint scanner for generating a first digitized fingerprint of the user, wherein the first digitized fingerprint of the user is compared with a second digitized fingerprint of the user stored in the encrypted data file.

17. (New) A system for authenticating an encryption key of a user, comprising:

an input device for receiving a password provided by the user;

memory for storing an encrypted data file including an encryption key of the user; and

a decrypt engine for using the password to decrypt the encrypted data file and thereby generating an authenticated encryption key of the user.

18. (New) The system of claim 17, wherein the encrypted data file is stored on an RF smart card.

19. (New) The system of claim 17, wherein the encrypted data file includes encrypted biometric data identifying the user.

20. (New) The system of claim 17, wherein the encrypted data file includes encrypted biometric data, derived from a digitized fingerprint of the user, identifying the user.

21. (New) The system of claim 17, further comprising a biometric reader for generating a first biometric data of the user, wherein the first biometric data of the user is compared with a second biometric data of the user stored in the encrypted data file.

22. (New) The system of claim 17, further comprising a fingerprint scanner for generating a first digitized fingerprint of the user, wherein the first digitized fingerprint of the user is compared with a second digitized fingerprint of the user stored in the encrypted data file.

23. (New) The system of claim 17, further comprising a server configured to receive data encrypted using the authenticated encryption key.

24. (New) A system for authenticating an encryption key of a user, comprising:

a input device for receiving a password provided by the user;

an RF smart card for storing an encrypted data file, the data file including an encryption key of the user;

a decrypt engine for using the password to decrypt the encrypted data file and thereby generate an authenticated encryption key of the user; and

memory for storing the decrypt engine.

25. (New) The system of claim 24, wherein the encrypted data file includes encrypted biometric data identifying the user.

26. (New) The system of claim 24, wherein the encrypted data file includes encrypted biometric data, derived from a digitized fingerprint of the user, identifying the user.

27. (New) A system for authenticating an encryption key of a user, comprising:

a input device for receiving a password provided by the user;

an RF smart card for storing an encrypted data file, the data file including an encryption key of the user and a first biometric data of the user;

a biometric reader for generating a second biometric data of the user; and

a decrypt engine for using the password to decrypt the encrypted data file, thereby generating an authenticated encryption key of the user, if there is a probabilistic match between the first biometric data and the second biometric data.

28. (New) A system for authenticating an encryption key of a user, comprising:

memory for storing an encrypted encryption key;

an input device for receiving a password;

a decrypt engine for using the password to decrypt the encrypted encryption key to an authenticated decrypted encryption key; and

memory for storing the decrypt engine.

29. (New) The system of claim 28, wherein the encrypted data file includes encrypted biometric data identifying the user.

30. (New) The system of claim 28, wherein the encrypted encryption key in is stored on an RF smart card.

31. (New) A system for authenticating an encryption key of a user, comprising:

memory for storing an encrypted encryption key and a first biometric data of the user;

an input device for receiving a password;

a biometric reader for generating a second biometric data of the user;

a decrypt engine for comparing the first biometric data of the user with a second biometric data of the user and, if there is a probabilistic match, then using the password to decrypt the encrypted encryption key to an authenticated decrypted encryption key; and

memory for storing the decrypt engine.

32. (New) The system of claim 31, wherein the password is used to decrypt the first biometric data before comparison with the second biometric data.

33. (New) The system of claim 31, wherein the biometric reader is a fingerprint scanner for generating a first digitized fingerprint of the user, and the first biometric data is a digitized fingerprint of the user.

34. (New) A method for authenticating an encryption key of a user, comprising the steps of:

storing an encrypted encryption key in memory;

receiving a password provided by a user; and

requiring use of the password to decrypt the encrypted encryption key to a decrypted encrypting key.

35. (New) The method of claim 34, wherein the encrypted encryption key is stored on an a RF smart card.

36. (New) The method of claim 34, wherein the encrypted encryption key is stored with encrypted biometric data identifying the user.

37. (New) The method of claim 36, wherein the encrypted biometric data includes a digitized fingerprint of the user.

38. (New) The system of claim 36, wherein the password is used to decrypt the first biometric data before comparison with the second biometric data.

39. (New) The method of claim 34, further comprising the steps of:

scanning a biometric feature of the user to generate first biometric data of the user;

decrypting second biometric data stored along with the encrypted encryption key;.

probabilistically comparing the generated first biometric data to the decrypted second biometric data; and

requiring the comparison to produce a probabilistic match before decrypting the encrypted encryption key to the decrypted encryption key.

40. (New) The method of claim 32, further comprising the step of reading the encrypted encryption key from an RF smart card.

41. (New) The method of claim 32, further comprising the step of using the decrypted encryption key to encrypt data.